**x) Schneier 2015: Applied Cryptography:**[**Chapter 1: Foundations**](https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/08_chap01.html#chap01-sec006)

**Secure Communication:**

* Sender sends a message securely to a receiver using encipher method.

**Encryption Basics:**

* Message (plaintext) is transformed into ciphertext for security.
* Decipher reverses this process to retrieve the original message.

**Cryptography Essentials:**

* Cryptography ensures secure message handling.
* Cryptanalysis involves breaking ciphertext.
* Cryptologists engage in cryptology (cryptography and cryptanalysis).

**y) Find out frequency distribution of letters for a language that you know (other than English). What are the six most common letters?**

In the Finnish language, the most frequently used letters, are typically:

1. A
2. I
3. T
4. N
5. E
6. S

Source: Matti Pääkkönen, ”A: sta ö:hön Suomen yleiskielen kirjaintilastoja”

**z) Choose a password manager. Explain:**

Bitwarden, an open-source password manager:

* **Threats Addressed:**
  + Bitwarden safeguards against password theft, phishing attacks, weak passwords, and unauthorized access, promoting secure password management.
* **Encrypted Information:**
  + All sensitive information, including passwords and notes, is end-to-end encrypted, ensuring user privacy and security.
* **License:**
  + Bitwarden operates under the GNU GPLv3 license, supporting software freedom, code accessibility, and community support.
* **Data Storage:**
  + Data is stored in Bitwarden's cloud servers, located in multiple data centers worldwide, prioritizing data privacy and compliance with relevant laws.
* **Data Protection:**
  + Strong end-to-end encryption (AES-256 bit) and salted hashing secure user data, with decryption and encryption processes occurring locally on users' devices for enhanced security. Multi-factor authentication (MFA) further improves protection.

1. ETAOIN. When asked to come up with encryption scheme in the class, almost everyone described a variation of a simple substitution chipher. As requested, now it's time to attack your own scheme! Crack this ciphertext:

* HDMH'B TH. KWU'YI AWR WSSTOTMJJK M OWQINYIMLIY! MB KWU BII, BTGPJI BUNBHTHUHTWA OTPDIYB OMA NI NYWLIA RTHD SYIEUIAOK MAMJKBTB. BII KWU MH DHHP://HIYWLMYCTAIA.OWG
* That’t it you’re now officially a codebreaker, as you see, simple substitution ciphers can be broken with sequency analysis. See you at http://terokarvinen.com

1. Demonstrate the use of a password manager.

A password manager like Bitwarden securely stores and manages passwords, generates strong passwords, and auto-fills credentials for easy access, enhancing online security and convenience.

1. Encrypt and decrypt a message. Explain the purpose of each step. Explain why you choose the tool you're using. (You can use any tool you want. You must do and report the encryption at the same time, it's not enough to try to remember what we did in the class. )
2. **Choosing the Encryption Tool:**
   * Manual substitution cipher for simplicity.
3. **Encryption:**
   * Secret key (letter mapping).
   * replace each letter in the message based on the key to create the encrypted message.
4. **Decryption:**
   * Secret key to reverse the substitution and decipher the message.

**Example:**

* **Original Message:** im ibrahim
* **Secret Key:** A -> Z, B -> Y, C -> X, D -> W, E -> V, F -> U, G -> T, H -> S, I -> R, J -> Q, K -> P, L -> O, M -> N, N -> M, O -> L, P -> K, Q -> J, R -> I, S -> H, T -> G, U -> F, V -> E,
* W -> D, X -> C, Y -> B, Z -> A,
* **Encrypted Message:** rn rzirzn
* **Decrypted Message:** Im ibrahim

**Purpose:**

* Ths encryption transforms the original message into a secret form (ciphertext) for security.
* Decryption reverses the encryption to obtain the original message.